File Storage Policy

Document Reference:	IT-POL-209
Document Classification:	Policy
Data Classification:	Public
Version number:	2.0
Relevant CIS Control(s):	Click or tap here to enter text.
Status:	Approved
Approved by (Board):	Information Governance Committee
Approval date:	22 October 2024
Effective from:	22 October 2024
Review Frequency:	Annual
Next review date:	22 October 2025
Document author:	IT Operations
Document owner:	Director of IT Operations
Contact:	IT Services
Collaborative provision:	**Yes**
Related documents:	
University document:	**No**
Published location:	**Sharepoint**

The University has adopted the principles of Designing for Diverse Learners, and all policy documents should be written with reference to these principles. Further information is available at the Designing for diverse learners website.

An Equality Impact Assessment (EIA) must be considered for all new and amended policies. Further information is available from the EIA section of SharePoint.

1 Table of Contents

2 Introduction

2.1 This policy outlines the use of file storage within the University to protect data.

2.2 This policy supports the objectives of the overarching **Information Security Controls Policy, as well as the Data Protection Policy, Data Breach Policy, Information Governance and Assurance Policy and the Data Classification and Handling Policy.**

3 Scope

3.1 This policy covers all devices used to conduct University related business, and any file storage methods

3.2 For the purposes of this policy, "University data" refers to any data owned or licensed by the University.

3.3 The University owns all data created by its employees unless it is created in a private capacity that is inconsequential to the employee's role. However, data that is created from research, which is paid for by an industry partner, sponsored or supported by an external funding source maybe exempt to this rule.

3.4 Data created by students during their studies or research will normally belong to the student, unless any of the following apply:

- The student receives a university studentship (a funded place on a programme), in which case ownership of the data will be decided in line with the terms of that studentship agreement.
- The student receives a bursary from, or have your fees paid or subsidised by, a sponsor, in which case the ownership of the data will be decided in line with the terms of the arrangement between the student, the University and the students sponsor.
- The data builds upon existing data created by the University or was jointly created by University employees or associates.
- The data builds upon existing data owned by a third party or was jointly created with a third party or University employees or associates.
- The student is an employee of the University and created the data in their role (in which case, see 3.3 above).

4 Local (fixed) disk drives

4.1 Local (fixed) disk drives (aka 'C: drive') on managed devices are for the primary purpose of storing the operating system and local profile settings for users of the device. These should always be regarded as volatile – when a managed device is imaged it **will** overwrite any data on it.

4.2 Local (fixed) disk drives **must not** be used for any storage of University or personal data. University data should always be stored on University network storage or approved University cloud storage services.

4.3 Local (fixed) disk drives **should not** be considered as secure.

4.4 IT Services will reserve the right to refuse any request to attempt restoration of any University or personal data that has been lost by having been stored on local (fixed) disk drives.

5 University Network storage

5.1 IT Services provide centralised network storage for all University members that may be hosted in University data centres or in third-party 'cloud' facilities. Network storage is subject to regular backup with a retention period of 18 months.

5.2 Network storage provided by the University is secured by authentication and access control, but not encrypted. This should be sufficient for business needs, however research data, for example, may have the need to be encrypted.

5.3 Network storage is subject to quotas and must only be used for storing University data, and not for the purpose of personal information such as photos, music, or videos.

5.4 A limited sized 'home' area is provided for device configuration that can only be accessed by the member of the University that it is provisioned for. Microsoft OneDrive (Cloud Storage) is the primary storage system for an individual.

5.5 Should a line manager require access to files held in a 'home' area that has been closed, they should submit an access request to the University Data Protection Officer. The request will be assessed and authorised in accordance with the University **Data Protection Policy**.

5.6 'Shared' storage areas can also be provided for departmental use upon request. Access to shared areas is controlled through centralised group membership mechanisms.

5.7 Each shared storage area must have a designated owner. This will either be the member requesting its creation, or a member to whom ownership has been transferred.

5.8 The designated owner of a shared storage area must agree to comply with the University **Data Protection and Data Classification & Handling Policies** and accept their responsibilities for its ongoing management.

5.9 The designated owner of a shared storage area is responsible for ensuring access is restricted to only authorised university members or known third parties; Research Collaborators for example. IT Services shall provide a suitable mechanism to allow the owner capability to administer group membership.

5.10 If a designated owner, or the line manager of that owner, needs to arrange cover for planned or unplanned absence, the owner or line manager should request temporary or permanent transfer of ownership or add an additional owner. This can be requested through IT Services. An additional or temporary owner will have the same levels of responsibility for the area as the original, designated owner.

5.11 If a University member assigned as owner changes role or leaves the institution, the line manager must ensure that ownership is transferred through a request to IT Services.

5.12 Should a shared area owner be assigned in error, the owner should contact IT Services.

5.13 All owners will be notified on a quarterly basis to review the current membership of each shared area for which they have responsibility.

5.14 University members must notify the University Data Protection Officer (via the Support Portal) if they know or suspect that any data has been breached or if data is inappropriate for shared areas. If personal data (PD[1]) is involved, the procedures in the **Data Protection Policy and Data Breach Policies** must be followed.

5.15 When a University member leaves the institution or changes to a role which no longer entitles them to a University Network storage account, their University Network storage account will be closed and then deleted after a period of 30 days.

[1] Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

6 Cloud storage

6.1 Only University approved cloud storage services should be used for the storing of University data. Details of University approved and provided cloud storage services can be found on the University Support Portal.

6.2 All University approved cloud storage will be encrypted storage.

6.3 Most University members are eligible for a University approved cloud storage account. Details of eligibility can be found on the University Support Portal.

6.4 Cloud storage allows for collaborative working. When sharing files, it is the responsibility of the storage area owner to check that the files are being shared with the intended collaborators.

6.5 Caution should always be exercised when sharing files through public links. These are not restricted to University members and anyone who is in possession of the link can access the shared files. This may not always be the intended recipient. To mitigate the risks of unintended sharing of files in this way IT Services have set the default expiry time of any shared public links to a period of 90 days.

6.6 If a University member changes role or leaves the institution and are an owner of files that have been previously shared, it is the responsibility of that member to ensure that ownership of files is transferred to another appropriate member before they do so.

6.7 When a University member leaves the institution or changes to a role which no longer entitles them to a cloud storage account, their cloud storage account will be closed and then deleted after a period of 30 days.

6.8 Should a line manager require access to files held in a cloud storage account that has been closed they should submit an access request to the University Data Protection Officer. The request will be assessed and authorised in accordance with the University **Data Protection Policy**.

6.9 Cloud storage is subject to quotas and must only be used for storing University data, and not for the purpose of personal information such as photos, music, or videos.

6.10 Wasabi data is held within a UK data centre and is not backed up. Alternative copies can be secured in another data centre if required.

6.11 Microsoft OneDrive, SharePoint and Exchange data is held within the UK whilst data for Teams is stored in the EU Zone.

6.12 If there is a need to store personal data (PD) on University approved cloud storage, then this must be done in accordance with the University **Data Protection Policy**.

6.13 University members must notify the University Data Protection Officer (via the Support Portal) if they know or suspect that any University data has been breached when using our approved cloud storage. If personal data (PD) is involved, the procedures in the University **Data Protection Policy and Data Breach Policies** must be followed.

7 Removable media

7.1 Removable media refers to any type of digital storage that is not physically fixed inside a device. This includes, but is not limited to: USB flash drives (aka 'memory sticks', pens), external hard disk drives, phones using SD card storage, and optical media (e.g. DVD, CD).

7.2 Removable media provide a common route for the introduction of malware and the accidental or deliberate export of sensitive data. In the normal course of business, it should not be necessary to use removable media, and the risk of doing so usually outweighs any perceived benefit.

7.3 Removable media is very easily lost, which can, and does, result in the breach of data.

7.4 Removable media that is used to transfer information from one device to another, for example a University PC to one at home, can be utilised by attackers to transport malicious software from one environment to the other.

7.5 Whilst the use of removable media within the University is not prohibited, it should only be used in cases where no suitable alternative exists (e.g. Network storage, shared areas or cloud storage).

7.6 Managers and information asset owners shall ensure that use of removable media is suitably controlled within their area of responsibility in line with the objectives of this policy.

7.7 University staff members within professional services electing to use removable media, shall be responsible for ensuring they are authorised to do so within their area.

7.8 Any removable media used by staff to transport or store any University data should be purchased via approved channels.

7.9 Personally owned removable media shall not be used by staff for the purposes of transporting or storing University data.

7.10 Data on removable media must be encrypted. Guidance on encryption including recommended hardware and software shall be available to University members from the Support Portal.

7.11 Researchers are responsible for ensuring that use of removable media and the encryption of any such media meets the requirements imposed upon them by their research (e.g. by funders, or data sharing agreements).

7.12 Use of removable media by third parties or sub-contractors should be risk-assessed and authorised, and in accordance with University **Data Protection Policy** governing third-party access to data.

7.13 It is recommended that removable media be made externally identifiable where possible (e.g. using a fob/tag or to note the owners name/contact number).

7.14 When the removable media has reached the end of its useful life it should be submitted to IT Services for secure destruction.

7.15 If removable media has been lost, it should be reported to Data protection in line with the University **Data Breach Policy**.

7.16 If removable media has been found, it should be handed in to the Campus Security team. If identifiable (from a description/external labelling) then attempts will be made to return to its owner. If this is not the case, removable media must never be inserted into a device to try and identify its owner, as this can present a security risk.

7.17 Any unidentifiable removable media that has not been claimed within six months will be submitted for secure destruction.

8 Responsible, Accountable, Consulted, and Informed (RACI) Matrix

8.1 A form of a responsibility assignment matrix (RAM) commonly used in project management[2]. A RACI matrix defines who is involved in the successful completion / implementation of a project, task, or in this case, a policy[3]. A brief definition of each role is given in the table below.

8.2 The table below outlines the roles that are involved in ensuring this policy is adhered to, enforced, and kept up to date.

[2] https://www.forbes.com/uk/advisor/business/software/raci-chart/
[3] https://project-management.com/understanding-responsibility-assignment-matrix-raci-matrix/

	Definition	Role
Responsible (R)	Answerable for the correct completion of the task	Director of IT Operations
Accountable (A)	Delegates and must sign off (approve) the work that those *responsible* provide	Executive Director Infrastructure Services
Consulted (C)	Provide input based on how this will impact their domain of expertise	IT Services
Informed (I)	Those who are kept up to date on progress	Information Governance Committee ULT

9 Version Control

Version	Author	Date approved	Relevant section(s)
1.0	Graeme Murphy	01/08/2023	All
1.1	Craig Stephenson	22/10/2024	All